NASA-CR-201863

NAGW-4013

The Applications of Generalized Bezout's Theorem to the Codes from the Curves in High Dimensional Spaces

Xiaofa Shi, Xinwen Wu, Gui-Liang Feng, and T. R. N. Rao*

July 16, 1996

Abstract

This paper generalizes the results in [1] to n-dimensional spaces.
For n-dimensional spaces, tighter upper bounds on the number of intersection points of two or more polynomials are given. Using the upper bounds, the lower bounds on the minimum distances and the generalized Hamming weights of linear codes defined on the curves in high dimensional spaces are obtained. For large enough h, the exact values of the generalized Hamming weights of linear codes defined on the curves in high dimensional spaces, $d_h(C_r)$, are given.
By using the generalized Bezoût theorem and the new approach, more efficient linear codes defined on the curves in high dimensional spaces are constructed, which are better than the AG codes and the improved AG codes on the same curves.

Index Terms: Bezout's theorem, minimum distance, generalized Hamming weights, algebraic-geometric codes, linear codes.

1 Introduction

For error-correcting codes, the minimum distance is one of most important parameters. It is used to measure the code's capacity of correcting errors or detecting errors or both [3]. The minimum distance d of a linear code C is defined by

$$d = \min_{\substack{\mathbf{u},\mathbf{v}\in C \\ \mathbf{u}\neq\mathbf{v}}} \{d(\mathbf{u},\mathbf{v})\},$$

where $d(\mathbf{u},\mathbf{v})$ expresses the Hamming distance between $\mathbf{u}$ and $\mathbf{v}$.

For an $[n,\ k]$ linear code, we can consider its generalized Hamming weights, which are the generalization of minimum distance and defined as follows:

*This work was supported in part by the National Science Foundation under Grant NCR-9505619, Louisiana Education Quality Support Fund under Grant LEQSF-(1994-96)-RD-A-36 and NASA Project NAG-W-4013.

Definition 1.1 *For any code C of block length n over $GF(q)$, define the* support $\mathcal{X}(C)$ *by*

$$\mathcal{X}(C) = \{i \mid c_i \neq 0 \ \textit{for some}\ (c_1, c_2, \cdots, c_n) \in C\},$$

and the support weight $w_s(C)$ *by*

$$w_s(C) = |\mathcal{X}(C)|.$$

Let C is a linear [n, k] code over $GF(q)$. For any r with $1 \leq r \leq k$, the r-th generalized Hamming weight *of C is defined as*

$$d_r(C) = \min\{w_s(D) \mid D \textit{ is a } r\textit{-dimensional subcode of } C\}.$$

The weight hierarchy of code C is defined as the set of generalized Hamming weights $\{d_1(C), d_2(C), \cdots, d_k(C)\}$.

It is easy to see that $d_1(C)$ is the minimum distance or the minimum Hamming weight of code C.

Let C be a q-ary $[n, k]$ linear code, we have the following properties of the generalized Hamming weights:

1) (Monotonicity) $1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n$.

2) (The generalized Singleton bound) $d_H(C) \leq n - k + h$, for $h = 1, 2, \cdots, k$.

These properties were proved for cases $q = 2$ in [4]. When q is a power of any prime, the proof is the same.

Both the determination of the minimum distances and the determination of weight hierarchy for linear codes in full are difficult. A more modest goal is to find acceptable bounds on these weights. The weights of geometric Goppa codes were discussed in [16] and [6]. The bounds on the minimum distance and the generalized Hamming weights of the codes defined on the curves in two-dimensional space were given in [1].

Definition 1.2 *Let $X = (x_1, x_2, \cdots, x_n)$, $D_{\{f_1, f_2, \cdots, f_p\}}$ denotes the number of distinct points of the intersection of polynomials $f_\mu(X) = 0$, for $\mu = 1, 2, ..., p$.*

Definition 1.3 *Given a sequence of polynomials $\{f_\mu(X) | \mu = 1, 2, ..., r\}$.*

$$D_p^{(r)} = \max\{D_{\{f^*_{\lambda_1}, f^*_{\lambda_2}, \cdots, f^*_{\lambda_p}\}} | \lambda_1, \cdots, \lambda_p \leq r\},$$

where $X = (x_1, x_2, \cdots, x_n)$ and $f^*_{\lambda_\mu}$ expresses a linear combination of f_i for i =1, 2, ..., λ_μ, and the coefficient of f_{λ_μ} is 1, i.e., $f^*_{\lambda_\mu} = f_{\lambda_\mu} + \sum_{i=1}^{\lambda_\mu - 1} c_i f_i$.

Let $LS = \{P_1, P_2, \cdots, P_N\}$ be a set of points in the n-dimensional vector space over $GF(q)$, in general, we consider the points in a algebraic curves, i.e., the rational points of a algebraic curve. Let $H_r = \{\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_r\}$ be a set of monomials or polynomials with variables $x_1, x_2, \cdots, x_n$. For every $\mathbf{h}_i$, we have a evaluated vector $(\mathbf{h}_i(P_1), \mathbf{h}_i(P_2), \cdots, \mathbf{h}_i(P_N))^T$. When there is no possibility of any confusion, we also use $\mathbf{h}_r$ to denote its evaluated vector, i.e., we let $\mathbf{h}_i = (\mathbf{h}_i(P_1), \mathbf{h}_i(P_2), \cdots, \mathbf{h}_i(P_N))^T$. Let C_r be the $[N, N - r]$ linear code defined by a parity check matrix $\mathbf{H}_r = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_r]^T$. The relationship between $D_p^{(r)}$ and the generalized Hamming weights of linear code C_r is given in the following theorem.

Theorem 1.1 *[1] For a linear code C_r defined by $\mathbf{H}_r$, i.e., the parity check matrix has r rows, if $D^{(r)}_{r-d^*+h+1} < d^* - 1$, then the h-th generalized Hamming weight $d_h(C_r)$ is at least d^*, i.e., $d_h(C_r) \geq d^*$.*

From the above theorem, we can see that an upper bound on the number of intersection points of two or more polynomials, $D^{(r)}_p$, can be used to obtain the lower bound on the generalized Hamming weight of a linear code. A generalized Bezout theorem is a good tool to determine the number of intersection points (common roots) of polynomials.

Definition 1.4 *Let $f_\mu(x,y)$, for $\mu = 1, 2, \cdots, p$, be polynomials in x and y. Without loss of the generality, $deg_x f_1 \geq deg_x f_2 \geq \cdots \geq deg_x f_p$, and let $deg_x f_1 = m$ and $deg_x f_2 = n$, where $deg_x f_\mu$ indicates the maximal i such that the monomial $x^i y^j$ is a term in f_μ. We define the x-resultant matrix of these p curves or polynomials as the following $\Sigma \times (m+n)$ matrix, where $\Sigma = \sum_{\mu=1}^{p} (m + n - deg_x f_\mu)$ and $s = deg_x f_p$:*

$$\begin{bmatrix}
a_0^{(1)} & a_1^{(1)} & \cdot & \cdot & \cdot & a_m^{(1)} & 0 & \cdot & \cdot & 0 \\
0 & a_0^{(1)} & a_1^{(1)} & \cdot & \cdot & \cdot & a_m^{(1)} & 0 & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & 0 & a_0^{(1)} & a_1^{(1)} & \cdot & \cdot & \cdot & a_m^{(1)} \\
a_0^{(2)} & a_1^{(2)} & \cdot & \cdot & a_n^{(2)} & 0 & 0 & \cdot & \cdot & 0 \\
0 & a_0^{(2)} & a_1^{(2)} & \cdot & \cdot & a_n^{(2)} & 0 & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & \cdot & \cdot & 0 & a_0^{(2)} & a_1^{(2)} & \cdot & a_n^{(2)} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_0^{(p)} & a_1^{(p)} & \cdot & \cdot & a_s^{(p)} & 0 & 0 & \cdot & \cdot & 0 \\
0 & a_0^{(p)} & a_1^{(p)} & \cdot & \cdot & a_s^{(p)} & 0 & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & \cdot & \cdot & 0 & a_0^{(p)} & a_1^{(p)} & \cdot & a_s^{(p)}
\end{bmatrix}.$$

Let $R(y) = Res_x(f_1, f_2, \cdots, f_p)$ be the non-zero determinant of nonsingular submatrix with the smallest degree of y of the x-resultant matrix. $R(y)$ is called the x-resultant of polynomials $f_1, f_2, \cdots$, and f_p.

Theorem 1.2 *[1] The number of distinct points of the intersection of $f_\mu(x,y)$ without common components, for $\mu = 1, 2, ..., p \geq n$, is at most equal to the degree of their resultant $R(y)$, i.e., $degR(y)$.*

For polynomials in n-dimensional spaces, we define the resultant by applying two-dimensional definition in the following way:

For $p \geq n$, consider the curve defined by

$$\left\{ \begin{array}{l} f_1(x_1, x_2, \cdots, x_n) = 0, \\ f_2(x_1, x_2, \cdots, x_n) = 0, \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ f_p(x_1, x_2, \cdots, x_n) = 0. \end{array} \right. \tag{1}$$

First, we consider the first two polynomials only.

$$\left\{ \begin{array}{l} f_1(x_1, x_2, \cdots, x_n) = 0, \\ f_2(x_1, x_2, \cdots, x_n) = 0. \end{array} \right.$$

If we consider x_1 and x_2 as the variables and $x_3, \cdots, x_n$ as parameters, then by applying the two-dimensional definition, we get the x_1-resultant $f_1^{(1)}(x_2, x_3, \cdots, x_n)$. Similarly, for $2 \leq i \leq p$, if we consider

$$\left\{ \begin{array}{l} f_1(x_1, x_2, \cdots, x_n) = 0, \\ f_i(x_1, x_2, \cdots, x_n) = 0. \end{array} \right.$$

we get an x_1-resultant $f_{i-1}^{(1)}(x_2, x_3, \cdots, x_n)$. After we get all the $p-1$ x_1-resultants, we consider the x_2-resultants $f_i^{(2)}(x_3, x_4, \cdots, x_n)$, for $i = 1, 2, \cdots, p-2$, of the following curve

$$\left\{ \begin{array}{l} f_1^{(1)}(x_2, x_3, \cdots, x_n) = 0, \\ f_2^{(1)}(x_2, x_3, \cdots, x_n) = 0, \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ f_{p-1}^{(1)}(x_2, x_3, \cdots, x_n) = 0. \end{array} \right.$$

Repeating the above procedure, we finally get $f_i^{(n-1)}(x_n)$, for $i = 1, \cdots, p-n+1$. We define the resultant of (1) as the one with minimum degree. In other words, we define $R(x_n) = f_{i_0}^{(n-1)}(x_n)$, where $deg f_{i_0}^{(n-1)}(x_n) \leq deg f_i^{(n-1)}(x_n)$ for $i = 1, \cdots, p-n+1$. The degree of $R(x_n)$ can be used to determine the number of the solutions of the system defined by (1).

Theorem 1.3 *The number of distinct points of the intersection of $f_\mu(x_1, x_2, \cdots, x_n)$ without common components, for $\mu = 1, 2, ..., p \geq n$, is at most equal to the degree of $R(x_n)$.*

In [1], a tighter bounds on $D_p^{(r)}$ were given for two dimensional polynomials by using a generalized Bezout theorem. With that upper bounds, lower bounds on the generalized Hamming weights of some linear codes were obtained. In this paper, we generalize the results in [1] to the general cases, n-dimensional cases.

In Section 2, we discuss some basic properties of polynomials and their common roots in n-dimensional Spaces. In Section 3, we concentrate on three dimensional spaces. In that section, the results in [1] will be generalized to three-dimensional spaces. The results in general n-dimensional Spaces will be given in Section 4. In Section 5, we construct some more efficient linear codes using generalized Bezout theorem and the results in Section 3. Conclusions are given in Section 6.

2 Basic Results for Polynomials in n-dimensional Spaces

In this section, we introduce some basic properties of n-dimensional polynomials. Throughout this section, X denotes a point in n-dimensional spaces, and $f(X), g(X)$ and f_μ denote polynomials in X.

For n-dimensional polynomials, we have the following results:

Proposition 2.1 *For any $f(X)$ and $g(X)$,*

$$D_{\{\cdots,f(X)g(X),\cdots\}} = D_{\{\cdots,f(X),\cdots\}} + D_{\{\cdots,g(X),\cdots\}} - D_{\{\cdots,f(X),\, g(X),\cdots\}}.$$

Proof: The set of all roots of $f(X)g(X) = 0$ is a union of the set of all roots of $f(X) = 0$ and the set of all roots of $g(X) = 0$. We have Proposition 2.1. □

Example 2.1 *Let $f(x,y) = x + y - 1, g(x,y) = xy$, and $h(x,y) = x - 1$. Consider*

$$\begin{cases} f(x,y)g(x,y) = xy(x+y-1) = 0, \\ h(x,y) = x - 1 = 0. \end{cases} \tag{2}$$

Obviously, system (2) has only one solution (1, 0). Thus, $D_{\{f(x,y)g(x,y),h(x,y)\}} = 1$.

Now, we consider the following systems

$$\begin{cases} f(x,y) = x + y - 1 = 0, \\ h(x,y) = x - 1 = 0. \end{cases} \tag{3}$$

$$\begin{cases} g(x,y) = xy = 0, \\ h(x,y) = x - 1 = 0. \end{cases} \tag{4}$$

and

$$\begin{cases} f(x,y) = x + y - 1 = 0, \\ g(x,y) = xy = 0. \end{cases} \tag{5}$$

It is easy to check that the three systems all have one solution. Therefore,

$$D_{\{f(x,y),h(x,y)\}} = 1, D_{\{g(x,y),h(x,y)\}} = 1, \text{ and } D_{\{f(x,y),g(x,y)\}} = 1.$$

Thus, we have

$$D_{\{f(x,y)g(x,y),h(x,y)\}} = D_{\{f(x,y),h(x,y)\}} + D_{\{g(x,y),h(x,y)\}} - D_{\{f(x,y),g(x,y)\}}.$$

Proposition 2.2 $D_{\{f_1,\cdots,f_p\}} \le \min\{D_{\{f_\mu\}} | \mu = 1, 2, ..., p\}$.

Proof: All the points of intersection of $f_\mu(X) = 0$, for $\mu = 1, 2, ..., p$, are the points of $f_\mu(X) = 0$, respectively. Therefore, we have Proposition 2.2. □

From Proposition 2.1 and Proposition 2.2, we have:

Proposition 2.3 $D_{\{gf_1,\cdots,gf_p\}} \le D_{\{g\}} + D_{\{f_1,\cdots,f_p\}}$.

Example 2.2 *Let $g(x) = x, f_1(x) = x^2 + x - 2$ and $f_2(x) = x^2 - x - 2$. Since system*

$$\begin{cases} g(x)f_1(x) = x(x^2 + x - 2) = 0, \\ g(x)f_2(x) = x(x^2 - x - 2) = 0 \end{cases}$$

has two solutions $x = 0$ and $x = 1$, we have $D_{\{gf_1,gf_2\}} = 2$. On the other hand, system

$$\begin{cases} f_1(x) = x^2 + x - 2 = 0, \\ f_2(x) = x^2 - x - 2 = 0 \end{cases}$$

has one solution $x = 1$. Thus, $D_{\{f_1,f_2\}} = 1$. Since $g(x) = x = 0$ has only one solution, we also have $D_{\{g\}} = 1$. Thus, we have

$$D_{\{gf_1,\cdots,gf_p\}} = D_{\{g\}} + D_{\{f_1,\cdots,f_p\}}.$$

If we take the same f_1 and f_2, but different g, say, $g(x) = x - 1$, then we can verify that

$$D_{\{gf_1,\cdots,gf_p\}} < D_{\{g\}} + D_{\{f_1,\cdots,f_p\}}.$$

Proposition 2.4 $D_{\{gf_1,f_1,\cdots,f_p\}} = D_{\{f_1,\cdots,f_p\}}$.

This result tells us that when consider the intersection points of some polynomials $g_1, g_2, \cdots, g_p$, if a polynomial g_i is the multiple of another polynomial g_j, then g_i can be deleted.

The following result can be used to simplify the procedure of determining the intersection points of polynomials.

Proposition 2.5 *For $i, k \geq 1$, $D_{\{\cdots,f(X)^i g(X)^k,\cdots\}} = D_{\{\cdots,f(X)g(X),\cdots\}}$.*

Proof: If $i = 1$ and $k = 1$, the result is trivial.

Suppose $i \geq 2$. From Proposition 2.1, we have

$$\begin{aligned} & D_{\{\cdots,f(X)^i g(X)^k,\cdots\}} \\ &= D_{\{\cdots,f(X),\cdots\}} + D_{\{\cdots,f(X)^{i-1}g(X)^k,\cdots\}} - D_{\{\cdots,f(X),f(X)^{i-1}g(X)^k,\cdots\}} \\ &= D_{\{\cdots,f(X)^{i-1}g(X)^k,\cdots\}} \\ &= \cdots \ \cdots \ \cdots \\ &= D_{\{\cdots,f(X)g(X)^k,\cdots\}}. \end{aligned}$$

If $k \geq 2$, similar to the above procedure, we have

$$\begin{aligned} & D_{\{\cdots,f(X)^i g(X)^k,\cdots\}} \\ &= D_{\{\cdots,f(X)g(X)^k,\cdots\}} \\ &= D_{\{\cdots,g(X),\cdots\}} + D_{\{\cdots,f(X)g(X)^{k-1},\cdots\}} - D_{\{\cdots,g(X),f(X)g(X)^{k-1},\cdots\}} \\ &= D_{\{\cdots,f(X)g(X)^{k-1},\cdots\}} \\ &= \cdots \ \cdots \ \cdots \\ &= D_{\{\cdots,f(X)g(X),\cdots\}}. \end{aligned}$$

□

Example 2.3 *Let $f(x,y,z) = x-1, g(x,y,z) = z, h_1(x,y,z) = y-1,$ and $h_2(x,y,z) = z-1$. Since system*

$$\begin{cases} f(x,y,z)g(x,y,z) = z(x-1) = 0, \\ h_1(x,y,z) = y-1 = 0, \\ h_2(x,y,z) = z-1 = 0, \end{cases}$$

has only one solution, we have

$$D_{\{fg,h_1,h_2\}} = 1.$$

Now, we consider

$$\begin{cases} f(x,y,z)^2 g(x,y,z)^2 = z^2(x-1)^2 = 0, \\ h_1(x,y,z) = y-1 = 0, \\ h_2(x,y,z) = z-1 = 0. \end{cases}$$

The above system also has only one solution. Therefore $D_{\{f^2g^2,h_1,h_2\}} = 1$. Thus,

$$D_{\{fg,h_1,h_2\}} = D_{\{f^2g^2,h_1,h_2\}}.$$

Proposition 2.6 $D^{(r)}_p \geq D^{(r)}_{p+1} + 1$.

Proof: Assume $D^{(r)}_{p+1} = D_{\{f^*_{\lambda_1}, f^*_{\lambda_2}, \dots, f^*_{\lambda_p}, f^*_{\lambda_{p+1}}\}}$, where $\lambda_{p+1} \leq r$. Let (X') not be in the intersection of the $p+1$ curves, i.e., $f_{\lambda_\mu}(X')$ are not all equal to zero, for $\mu = 1, 2, \dots, p, p+1$. Without loss of the generality, let $f^*_{\lambda_1}(X') \neq 0$. We denote $f^*_{\lambda_\mu}(X') = v_\mu$ for $\mu = 1, 2, \dots, p, p+1$. Thus, $v_1 \neq 0$. Now we define $f'_{\lambda_\mu} = f^*_{\lambda_\mu} - \frac{v_\mu}{v_1} f^*_{\lambda_1}$, for $\mu = 2, 3, \dots, p, p+1$. Thus, we have $f'_{\lambda_\mu}(X') = 0$ for $\mu = 2, 3, \dots, p,$ $p+1$. It is easily seen that if $f^*_{\lambda_\mu}(X^*)$ $= 0$ for $\mu = 1, 2, 3, \dots, p, p+1$, then $f'_{\lambda_\mu}(X^*) = 0$ for $\mu = 2, 3, \dots, p, p+1$. Therefore, $D_{\{f'_{\lambda_2}, \dots, f'_{\lambda_p}, f'_{\lambda_{p+1}}\}} \geq D^{(r)}_{p+1} + 1$. From the definition of $D^{(r)}_p$, we have $D^{(r)}_p \geq D^{(r)}_{p+1} + 1$. The proof is completed. □

Remark 2.1: Proposition 2.6 corresponds to the monotonicity of the generalized Hamming weights.

Proposition 2.7 *If $\mathbf{h}_{r+1} = f^l g$, where $l \geq 2$ and deg $f \geq 1$. Then*

$$D^{(r+1)}_p \leq D^{(r)}_p.$$

Proof: Let $D^{(r+1)}_p = D_{\{\mathbf{h}^*_{s_1}, \dots, \mathbf{h}^*_{s_{p-1}}, \mathbf{h}^*_{s_p}\}}$. When $\mathbf{h}^*_{s_p} \neq \mathbf{h}_{r+1}, s_p \leq r$, we have

$$D^{(r+1)}_p = D_{\{\mathbf{h}^*_{s_1}, \dots, \mathbf{h}^*_{s_{p-1}}, \mathbf{h}^*_{s_p}\}} \leq D^{(r)}_p.$$

When , $\mathbf{h}_{s_p} = \mathbf{h}_{r+1} = f^l g$, from Proposition 2.5, we have

$$\begin{aligned} D^{(r+1)}_p &= D_{\{\mathbf{h}^*_{s_1}, \dots, \mathbf{h}^*_{s_{p-1}}, (f^l g)^*\}} \\ &= D_{\{\mathbf{h}^*_{s_1}, \dots, \mathbf{h}^*_{s_{p-1}}, (fg)^*\}} \\ &\leq D^{(r)}_p. \end{aligned}$$

□

3 The Generalized Hamming Weights of AG Codes from a Class of Three-dimensional Curves

We are now interested in the following irreducible space curves [9, 10]:

$$\begin{cases} x^a + y^b + f_1(x,y) = 0, \\ y^a + z^b + f_2(x,y,z) = 0, \end{cases} \tag{6}$$

where $gcd(a,b) = 1$, and $b^2 i + abj + b^2 k < ab$ for any $x^i y^j z^k$ being a term in $f_i(x,y,z)$. Miura-Kamiya space curves are special cases of (6) [11]. Since they are irreducible, any set containing one of these polynomials has no common non-constant factor. The results of this section can be generalized to the space curves of (6), but for convenience of exposition we derive them using the following Hermitian space curve over $GF(2^4)$ as an example:

$$\begin{cases} x^5 + y^4 + y = 0, \\ y^5 + z^4 + z = 0. \end{cases} \tag{7}$$

For (7), we define the weights of monomials as follows: $w(x) = 16$, $w(y) = 20$, $w(z) = 25$ and $w(x^i y^j z^k) = 16i + 20j + 25k$. We have the following sequence of monomials:

$H = \{\ 1,\ x,\ y,\ z,\ x^2,\ xy,\ y^2, xz,\ yz,\ x^3\ , z^2,\ x^2y,\ xy^2,\ x^2z,\ y^3,\ xyz,\ x^4, y^2z,\ xz^2,\ x^3y,\ yz^2,\ x^2y^2,\ x^3z,\ z^3, xy^3,\ \ldots\ \} = \{\ x^i y^j z^k | 0 \le i \le 15, 0 \le j \le 3, 0 \le k \le 3\} = \{\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \ldots, \mathbf{h}_r, \ldots, \mathbf{h}_{256}\ \}$.

It can be checked that the weights of monomials in H form an ascending sequence: $W = \{0, 16, 20, 25, 32, 36, 40, 41, 45, 48, \ldots, 350, 355, 359, 375\}$.

Let $L(r)$ be the linear space spanned by the first r monomials of H. Obviously $\mathbf{h}_r \in L(r) - L(r-1)$. If polynomials $f(x,y,z)$, $g(x,y,z) \in L(r) - L(r-1)$, we say $f(x,y,z)$ and $g(x,y,z)$ are *consistent* and write $f(x,y,z) \sim g(x,y,z)$. In this paper, $[x^i y^j z^k]$ (or $\mathbf{h}_r^*$) denotes all polynomials that are linear combinations of $x^i y^j z^k$ (or $\mathbf{h}_r$) and its previous monomials in which the coefficient of $x^i y^j z^k$ (or $\mathbf{h}_r$) is 1, i.e., $\mathbf{h}_r^* \equiv \mathbf{h}_r + \sum_{\mu=1}^{r-1} c_\nu \mathbf{h}_\mu$. Hence we have $[x^i y^j z^k] \sim x^i y^j z^k$ and $\mathbf{h}_r^* \sim \mathbf{h}_r$. For convenience, let $\mathbf{h}_0 = x^5 + y^4 + y$. Sometimes, if no confusion arises, $D_{\{\mathbf{h}_{\lambda_1}^*, \mathbf{h}_{\lambda_2}^*, \cdots, \mathbf{h}_{\lambda_p}^*\}}$ is represented as $D_{\{\lambda_1, \lambda_2, \cdots, \lambda_p\}}$. From these definitions and the results in Section II, we have the following lemmas.

Lemma 3.1 $D_{\{[x^i y^j z^k]\}} \le 16i + 20j + 25k$.

Proof: Let $\mathbf{h}_r = x^i y^j z^k$ and consider any linear combination of the form $\mathbf{h}_r^* = x^i y^j z^k + \sum_{\mu=1}^{r-1} c_\mu \mathbf{h}_\mu$. Each monomial $\mathbf{h}_\mu$, $1 \le \mu < r$, has a y-exponent at most 3. Thus, $x^5 + y^4 + y$ is not a factor of $\mathbf{h}_r^*$. Since $x^5 + y^4 + y$ is irreducible, $\mathbf{h}_r^*$ and $x^5 + y^4 + y$ have no common factors. So Theorem 1.2 applies.

The *x-resultant* $R(y)$ of $x^5 + y^4 + y = 0$ and $x^i y^j z^k + \cdots = 0$ is the determinant of the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & y^4+y & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & y^4+y & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & y^4+y & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 0 & \ldots & y^4+y \\ y^jz^k & a(y,z) & b(y,z) & \ldots & c(y,z) & 0 & 0 & \ldots & 0 & 0 \\ 0 & y^jz^k & a(y,z) & b(y,z) & \ldots & c(y,z) & 0 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \ldots & y^jz^k & a(y,z) & \ldots & c(y,z) \end{bmatrix},$$

where $deg_y\ a(y,z), deg_y\ b(y,z), ..., deg_y\ e(y,z)$ are all less than 4. Thus,

$$R(y,z) = (y^jz^k)^5(y^4+y)^i + \cdots = y^{4i+5j}z^{5k} + \cdots.$$

Now, consider the $y-resultant$ $R(z)$ of $y^5+z^4+z=0$ and $y^{4i+5j}z^{5k}+\cdots$. From Theorem 1.2, $R(z)$ is the determinant of the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & z^4+z & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & z^4+z & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & z^4+z & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 0 & \ldots & z^4+z \\ z^{5k} & a(y,z) & b(y,z) & \ldots & c(y,z) & 0 & 0 & \ldots & 0 & 0 \\ 0 & z^{5k} & a(y,z) & b(y,z) & \ldots & c(y,z) & 0 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \ldots & z^{5k} & a(y,z) & \ldots & c(y,z) \end{bmatrix},$$

Thus,

$$R(z) = z^{4(4i+5j)+5(5k)} + \cdots = z^{16i+20j+25k} + \cdots,$$

and therefore, $degR(z) = 16i+20j+25k$. The proof is completed. □

Lemma 3.2 *Let* $gcd(\mathbf{h}_{\lambda_1}, ..., \mathbf{h}_{\lambda_p}) = \mathbf{h}$. *Then*

$$D_{\{\mathbf{h}^*_{\lambda_1},...,\mathbf{h}^*_{\lambda_p}\}} \leq D_{\{\mathbf{h}\}} + D_{\{[x^{i_1}y^{j_1}z^{k_1}],...,[x^{i_t}y^{j_t}z^{k_t}]\}},$$

where $0 \leq i_1, i_2, \cdots, i_t \leq 4$, $0 \leq j_1, j_2, \cdots, j_t \leq 3$, *and* $0 \leq k_1, k_2, \cdots, k_t \leq 3$.

Proof: Since $y^4 = x^5+y$ and $z^4 = y^5+z$, and applying Proposition 2.3 and Proposition 2.4, we have Lemma 3.2. □

Example 3.1 *Let* $\mathbf{h}_{\lambda_\mu}$, *for* $\mu = 1, 2, ..., 6$, *be* x^6yz^2, x^5yz, $x^3y^2z^2$, x^4y^2z, $x^2y^2z^3$, xy^2z^2. *Thus,* $gcd(x^6yz^2, x^5yz, x^3y^2z^2, x^4y^2z, x^2y^2z^3, xy^2z^2) = xyz$, *i.e.,* $\mathbf{h} = xyz$. *From Proposition 2.4,* $x^6yz^2, x^3y^2z^2$, *and* $x^2y^2z^3$ *can be deleted. Thus, from Lemma 3.2, we have*

$$D_{\{[x^6yz^2],[x^5yz],[x^3y^2z^2],[x^4y^2z],[x^2y^2z^3],[xy^2z^2]\}} \le D_{\{[xyz]\}} + D_{\{[x^4],[x^3y],[yz]\}}.$$

Definition 3.1 *Let* i, j *and* k *are nonnegative integers. The determine set of a point* $p = (i, j, k)$ *is defined as*

$$\mathcal{D}(i,j,k) = \mathcal{D}(p) = \{(i',j',k') \mid \begin{array}{l} (0 \le i' \le \min\{i-1, 15\}, 0 \le j' \le 3, 0 \le k' \le 3) \text{ or} \\ (0 \le i' \le \min\{i+4, 15\}, 0 \le j' < \min\{j, 4\}, 0 \le k' \le 3) \text{ or} \\ (0 \le i' \le \min\{i+4, 15\}, 0 \le j' \le 3, 0 \le k' < \min\{k, 4\})\}. \end{array}$$

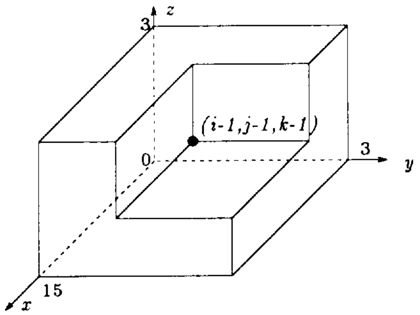

Figure 2.1 The determine set of point *p=(i, j, k)*.

Let $P_1, P_2, \cdots, P_n$ *be* n *points with nonnegative coordinators. The determine set of the* n *points is defined as*

$$\mathcal{D}(P_1, P_2, \cdots, P_m) = \mathcal{D}(P_1) \cap \mathcal{D}(P_2) \cap \cdots \cap \mathcal{D}(P_n).$$

Theorem 3.1 *Let* $P_t = (i_t, j_t, k_t)$, *for* $t = 1, 2, \cdots, n$. *Then*

$$D_{\{[x^{i_1}y^{j_1}z^{k_1}],\ldots,[x^{i_n}y^{j_n}z^{k_n}]\}} \le |\mathcal{D}(P_1, P_2, \cdots, P_n)|,$$

where $|\mathcal{D}(P_1, P_2, \cdots, P_n)|$ *is the number of points in* $\mathcal{D}(P_1, P_2, \cdots, P_n)$, *and* $t \le 4, 0 \le i_t \le 15$, $0 \le j_t \le 3$, *and* $0 \le k_t \le 3$.

It may be difficult to give an explicit formula for computing $|\mathcal{D}(P_1, P_2, \cdots, P_n)|$. Here, we give a simple algorithm that is easy to implement.

Algorithm 3.1 *(Computation of* $|\mathcal{D}|$*) Suppose* $\mathcal{D} = \mathcal{D}(P_1, P_2, \cdots, P_n)$ *and* $P_t = (i_t, j_t, k_t)$.

```
Step 1: Set $\mathcal{D}_0 := \{(i,j,k) \mid 0 \le i \le 15, 0 \le j \le 3, 0 \le k \le 3\}$.

Step 2: For $t = 1, 2, \cdots, n$, do

            For $i_t \le i \le 15, i_t \le j \le 3, k_t \le k \le 3$ do

              If $(i,j,k) \in \mathcal{D}_0$, then
```

```
        $\mathcal{D}_0 := \mathcal{D}_0 - (i,j,k)$.
    For $\min\{i_t+4,15\} < i \le 15, 0 \le j \le 3, 0 \le k \le 3$ do
        If $(i,j,k) \in \mathcal{D}_0$, then
        $\mathcal{D}_0 := \mathcal{D}_0 - (i,j,k)$.
```

Step 3: $|\mathcal{D}| =$ *the number of points in* $\mathcal{D}_0$.

Example 3.2 *Using Algorithm 3.1, we have*

$$D_{\{[x^4z^2],[x^2y],[y^2z]\}} \le 30.$$

Lemma 3.3 *If* $D_p^{(r)} = D_{\{s_1,s_2,...,s_p\}}$ *and* $\mathbf{h}_{t_\lambda}$ *is deleted, i.e.,* $t_\lambda \in \{1,2,...,r\} - \{s_1,s_2,...,s_p\}$, *then all factors of* $\mathbf{h}_{t_\lambda}$ *should be deleted, i.e., it is not in the set* $\{\mathbf{h}_{s_1},...,\mathbf{h}_{s_p}\}$.

Proof: Suppose that

$$D_p^{(r)} = D_{\{s_1,s_2,...,s_p\}}.$$

Let $\{t_1,t_2,...,t_{r-p}\} = \{1,2,...,r\} - \{s_1,s_2,...,s_p\}$. If $\mathbf{h}_{s_\mu}$ is a factor of $\mathbf{h}_{t_\lambda}$, then from Proposition 2.4 and the definitions, we have

$$D_p^{(r)} = D_{\{s_1,s_2,...,s_p\}} = D_{\{s_1,s_2,...,s_p,t_\lambda\}} \le D_{p+1}^{(r)}.$$

However, from Proposition 2.6, we have $D_p^{(r)} \ge D_{p+1}^{(r)} + 1$. Thus, we have a contradiction.
□

Definition 3.2 *A set* S *of non-negative integer points* (i,j,k) *(i.e.,* i, j *and* k *are non-negative integers) is called a regular set if for* $(i,j,k) \in S$, *we have* $(i',j',k') \in S$, *for all* $0 \le i' \le i$, $0 \le j' \le j$ *and* $0 \le k' \le k$.

Using the definition, we have the following result:

Corollary 3.1 *For* $D_{\{k_1,k_2,...,k_p\}}$, *if set* $\{(i,j,k)|x^iy^jz^k \in \{\mathbf{h}_1,\mathbf{h}_2,...,\mathbf{h}_r\} - \{\mathbf{h}_{k_1},\mathbf{h}_{k_2},...,\mathbf{h}_{k_p}\}\}$ *is not a regular set, then there exists at least one set of* $\{s_1,s_2,...,s_p\}$ *with* $s_p \le k_p$, *such that* $D_{\{s_1,s_2,...,s_p\}} \ge 1 + D_{\{k_1,k_2,...,k_p\}}$.

Example 3.3 *Let* $r = 14$ *and* $p = 6$. *The first 14 monomials are* { *1,* x, y, z, x^2, xy, y^2, xz, yz, x^3 ,z^2, x^2y, xy^2, y^3 }. *If* { k_1, ..., k_6 } = { *2, 7, 11, 12, 13, 14* }, *then* $\{1,2,...,r\} - \{k_1,...,k_p\} = \{1,3,4,5,6,8,9,10\}$. *Observe the set* $\{(i,j,k)|x^iy^jz^k \in \{\mathbf{h}_1,\mathbf{h}_3,\mathbf{h}_4,\mathbf{h}_5,\mathbf{h}_6,\mathbf{h}_8,\mathbf{h}_9,\mathbf{h}_{10}\}\}$ = { (0,0,0), (0,1,0), (0,0,1), (2,0,0), (1,1,0), (0,2,0), (0,1,1), (3,0,0) } *does not form a regular set, because* $(2,0,0)$ *belongs to this set but (1,0,0) does not. If we choose* $\{s_1,...,s_6\} = \{7,9,11,12,13,14\}$, *then* $\{1,2,...,r\} - \{s_1,...,s_p\} = \{1,2,3,4,5,6,8,10\}$. *The corresponding monomials are* {*1,* x, y, z, x^2, xy, xz,x^3 } *and form a regular set. Obviously,* $D_{\{7,9,11,12,13,14\}} \ge 1 + D_{\{2,7,11,12,13,14\}}$.

The following theorem is the main results of this paper.

Theorem 3.2 $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p)$.

Proof: We use mathematical induction here.
(1) For $\mathbf{h}_r = 1, x, y, z, x^2, xy, y^2, xz, yz$, it can be checked directly that

$$D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p).$$

(2) Suppose $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p)$ holds for $r \leq 9$. Since $\mathbf{h}_{r+1} = f^2 g$ for some f and g when $9 \leq r \leq 14$. By Proposition 2.7, we have

$$D_p^{(r+1)} \leq D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p) \leq w(\mathbf{h}_{r+1}) - w(\mathbf{h}_p).$$

(3) Now, suppose that $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p)$ for $r \leq 15$. We prove that $D_p^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p)$.

Let $D_p^{(16)} = D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},\mathbf{h}^*_{s_p}\}}$. If $s_p \leq 15$, then

$$D_p^{(16)} = D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},\mathbf{h}^*_{s_p}\}} \leq D_p^{(15)} \leq w(\mathbf{h}_{15}) - w(\mathbf{h}_p) \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p).$$

If $s_p = 16$, $D_p^{(16)} = D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(xyz)^*\}}$. We distinguish further the following cases.

(i) $w(\mathbf{h}_{s_{p-1}}) \leq w(yz)$.

$$\begin{aligned}
D_p^{(16)} &= D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(xyz)^*\}} \\
&\leq D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(yz)^*\}} + D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(x)^*\}} \\
&\leq D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(yz)^*\}} + D_{\{x^*\}} \\
&\leq D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},(yz)^*\}} + w(x) \\
&= w(yz) - w(\mathbf{h}_p) + w(x) \\
&\leq w(xyz) - w(\mathbf{h}_p) \\
&= w(\mathbf{h}_{16}) - w(\mathbf{h}_p).
\end{aligned}$$

(ii) $w(\mathbf{h}_{s_{p-1}}) > w(yz)$, then $\mathbf{h}_{s_{p-1}} = x^3, z^2, x^2y, xy^2, x^2z, y^3$. Without loss of generality, we take $\mathbf{h}_{s_{p-1}} = y^3$. Then

$$\begin{aligned}
D_p^{(16)} &= D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},(y^3)^*,(xyz)^*\}} \\
&= D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},y^*,(xyz)^*\}} \\
&= D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},y^*\}}.
\end{aligned}$$

In order to prove $D_p^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p)$, we need to prove

$$D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},y^*\}} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p). \tag{8}$$

If $\mathbf{h}_{s_i} = 1$ for some s_i, then

$$D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},y^*\}} = 0 \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p).$$

If there are some $\mathbf{h}_{s_i}, \mathbf{h}_{s_j}$, such that $\mathbf{h}_{s_i} = x, \mathbf{h}_{s_j} = z$, then

$$D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-2}},y^*\}} = D_{\{\cdots,x^*,\cdots,y^*,\cdots,y^*\}} = 1 \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p).$$

And when $p = 1, D_1^{(16)} \leq w(\mathbf{h}_{16}) = w(\mathbf{h}_{16}) - w(\mathbf{h}_1)$. When $p = 15$, $\{\mathbf{h}_{s_1}, \cdots, \mathbf{h}_{s_{14}}\} \subset \{\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_{15}\}$. Therefore, either there is a $\mathbf{h}_{s_i} = 1$ or there are some $\mathbf{h}_{s_i} = x$ and $\mathbf{h}_{s_j} = z$. For either cases, we have $D_p^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p)$.

Now by Proposition 2.4, we can delete the terms, which have y as a factor, from $D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},y^*\}}$. Thus, we can assume that

$$D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},y^*\}} = D_{\{x^*,y^*\}} \text{ or } D_{\{z^*,y^*\}}.$$

Hence $D_{\{\mathbf{h}^*_{s_1},\cdots,\mathbf{h}^*_{s_{p-1}},y^*\}} = 4 \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{14}) \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p)$.

Combining (i) and (ii), we have proved that

$$D_p^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_p).$$

(4) We now prove that when $r > 15$, $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p)$.

When $r > 15$, $\mathbf{h}_{r+1} = f^2 g$ for some f and g. By Proposition 2.7,

$$D_p^{(r+1)} \leq D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p) \leq w(\mathbf{h}_{r+1}) - w(\mathbf{h}_p).$$

Thus, the proof is completed. □

Corollary 3.2 *If* $\mathbf{h}_r \sim \mathbf{h}_p \cdot \mathbf{h}_\mu$ *for some* $1 \leq \mu < r$, *and* $D_{\{\mathbf{h}^*_\mu\}} = w(\mathbf{h}_\mu)$, *then*

$$D_p^{(r)} = w(\mathbf{h}_\mu).$$

Proof: Since $\mathbf{h}_r \sim \mathbf{h}_p \cdot \mathbf{h}_\mu$,

$$\mathbf{h}_\mu \times \{\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_p\} \subseteq \{\mathbf{h}_1, \cdots, \mathbf{h}_p, \cdots, \mathbf{h}_r\}.$$

Thus, by Proposition 2.3, $D_p^{(r)} \geq D_{\{\mathbf{h}^*_\mu \mathbf{h}^*_1, \mathbf{h}^*_\mu \mathbf{h}^*_2, \cdots, \mathbf{h}^*_\mu \mathbf{h}^*_p\}} \geq D_{\{\mathbf{h}^*_\mu\}}$.

On the other hand, $D_{\{\mathbf{h}^*_\mu\}} = w(\mathbf{h}_\mu) = w(\mathbf{h}_r) - w(\mathbf{h}_p)$. From Theorem 3.2, $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p) = D_{\{\mathbf{h}^*_\mu\}}$. Therefore, $D_p^{(r)} = D_{\{\mathbf{h}^*_\mu\}} = w(\mathbf{h}_\mu)$.

Lemma 3.4 *[1] If there is no* $1 \leq \mu < r$ *such that* $\mathbf{h}_r \sim \mathbf{h}_p \cdot \mathbf{h}_\mu$, *and* $r - p \geq w(\mathbf{h}_\nu)$, *for any* $1 \leq \nu < r$ *with that* $\mathbf{h}_{r'} \sim \mathbf{h}_p \cdot \mathbf{h}_\nu$ *and* $r' \leq r$, *then*

$$D_p^{(r)} \leq r - p. \tag{9}$$

Now we show how to find the generalized Hamming weights of codes C_r defined by $\mathbf{H}_r$. For convenience of expression, we take $r = 16$. For

$$\mathbf{H}_{16} = [1, x, y, z, x^2, xy, y^2, xz, yz, x^3, z^2, x^2y, xy^2, x^2z, y^3, xyz]^T,$$

we have the following table:

μ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathbf{h}_\mu$	1	x	y	z	x^2	xy	y^2	xz	yz	x^3	z^2	x^2y	xy^2	x^2z	y^3	xyz
$w(\mathbf{h}_\mu)$	0	16	20	25	32	36	40	41	45	48	50	52	56	57	60	61

Table 1: The weights for the first 16 monomials.

With Table 1 and Theorem 3.3, we compute

$D_1^{(16)} = w(\mathbf{h}_{16}) = 61$ $\quad D_2^{(16)} = w(\mathbf{h}_9) = 45$ $\quad D_3^{(16)} = w(\mathbf{h}_8) = 41$
$D_4^{(16)} = w(\mathbf{h}_6) = 36$ $\quad D_5^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_5) = 29$ $\quad D_6^{(16)} = w(\mathbf{h}_4) = 25$
$D_7^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_7) = 21$ $\quad D_8^{(16)} = w(\mathbf{h}_3) = 20$ $\quad D_9^{(16)} = w(\mathbf{h}_{12}) = 16$
$D_{10}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{10}) = 13$ $\quad D_{11}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{11}) = 11$ $\quad D_{12}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{12}) = 9$
$D_{13}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{13}) = 5$ $\quad D_{14}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{14}) = 4$ $\quad D_{15}^{(16)} \leq w(\mathbf{h}_{16}) - w(\mathbf{h}_{15}) = 1$
$D_{16}^{(16)} = 0$

Now using the monotonicity proposition, i.e. Proposition 2.6, we obtain $D_7^{(16)} = 21$.

	d - 1 = 16 - p + h												
p	h=1	h=2	h=3	h=4	h=5	h=6	h=7	h=8	h=9	h=10	h=11	h=12	$D_p^{(16)}$
1	16	17	18	19	20	21	22	23	24	25	26	27	61
2	15	16	17	18	19	20	21	22	23	24	25	26	45
3	14	15	16	17	18	19	20	21	22	23	24	25	41
4	13	14	15	16	17	18	19	20	21	22	23	24	36
5	12	13	14	15	16	17	18	19	20	21	22	23	≤ 29
6	11	12	13	14	15	16	17	18	19	20	21	22	25
7	10	11	12	13	14	15	16	17	18	19	20	21	21
8	9	10	11	12	13	14	15	16	17	18	19	20	20
9	8	9	10	11	12	13	14	15	16	17*	18*	19*	16
10	7*	8*	9*	10*	11*	12*	13*	14*	15*	16	17	18	≤ 13
11	6*	7*	8*	9*	10*	11*	12*	13	14	15	16	17	≤ 11
12	5*	6*	7*	8*	9*	10*	11	12	13	14	15	16	≤ 9
13	4*	5*	6*	7*	8*	9	10	11	12	13	14	15	≤ 5
14	3*	4*	5	6	7	8	9	10	11	12	13	14	≤ 4
15	2*	3*	4	5	6	7	8	9	10	11	12	13	1
16	1	2	3	4	5	6	7	8	9	10	11	12	0

Table 2: The values of d-1=16-p+h for different h and p.

With Table 2 and Table 3, we can compute the generalized Hamming weights, $d_i(C_{16})$, or their bounds as follows. From the table, for each column $h = i$ (i = 1, 2, 3, 4, ...), we consider the first entry that is greater than the entry at the same row and the last column($D_p^{(16)}$). According to Theorem 1.1, this entry plus 1 gives a lower bound of $d_i(C_{16})$. However, for some p (such as $p = 5, p = 10, \cdots, p = 14$), we only have the bounds on $D_p^{(16)}$. Thus, there may be more than one entry in one column that are possible to be the first entry

	d - 1 = 16 - p + h												
p	h=13	h=14	h=15	h=16	h=17	h=18	h=19	h=20	h=21	h=22	h=23	h=24	$D_p^{(16)}$
1	28	29	30	31	32	33	34	35	36	37	38	39	61
2	27	28	29	30	31	32	33	34	35	36	37	38	45
3	26	27	28	29	30	31	32	33	34	35	36	37	41
4	25	26	27	28	29	30	31	32	33	34	35	36	36
5	24	25	26	27*	28*	29*	30*	31*	32*	33*	34*	35*	≤ 29
6	23	24	25	26*	27*	28*	29	30	31	32	33	34	25
7	22*	23*	24*	25	26	27	28	29	30	31	32	33	21
8	21	22	23	24	25	26	27	28	29	30	31	32	20
9	20	21	22	23	24	25	26	27	28	29	30	31	16
10	19	20	21	22	23	24	25	26	27	28	29	30	≤ 13
11	18	19	20	21	22	23	24	25	26	27	28	29	≤ 11
12	17	18	19	20	21	22	23	24	25	26	27	28	≤ 9
13	16	17	18	19	19	21	22	23	24	25	26	27	≤ 5
14	15	16	17	18	18	20	21	22	23	24	25	26	≤ 4
15	14	15	16	17	17	19	20	21	22	23	24	25	1
16	13	14	15	16	16	18	19	20	21	22	23	24	0

Table 3: The values of d-1=16-p+h for different h and p (continued).

that is greater than the value of $D_p^{(16)}$. In Table 2 and Table 3, all these entries are marked by an '*'. For the same reason, in Table 4, we only give the bounds of the generalized Hamming weights for some h.

The generalized Hamming weights of C_{16} are given in Table 4.

h	1	2	3	4	5	6	7	8	9	
$d_h(C_{16})$	[3,8]	[4,9]	[7,10]	[8,11]	[9,12]	[11,13]	[13,14]	15	16	
h	10	11	12	13	14	15	16	17	18	19
$d_h(C_{16})$	18	19	20	23	24	25	[27,28]	[28,29]	[29,30]	31
h	[20,24]		[25,28]		[29,32]		[33,46]		[47,256]	
$d_h(C_{16})$	h+12		h+13		h+14		h+15		h+16	

Table 4: The generalized Hamming weights of C_{16}.

In Table 4, $h \in [a,b]$ or $d_h(C_{16}) \in [a,b]$ means that h or $d_h(C_{16})$ may take any integer in the interval $[a,b]$.

4 Results in General n-dimensional Spaces

In this section, we consider the codes defined on the curves in n-dimensional space. We are now interested in the following irreducible space curves [2]:

$$\begin{cases} f(x_1, x_2) = 0, \\ f(x_1, x_2, x_3) = 0, \\ \cdots\ \cdots\ \cdots\ \cdots \\ f_{n-1}(x_1, x_2, \cdots, x_n) = 0, \end{cases} \tag{10}$$

where

$$f_s((x_1, x_2, \cdots, x_{s+1}) = x_s^{a_s} + x_{s+1}^{b_s} + g_s(x_1, x_2, \cdots, x_{s+1}),$$

$$gcd(a_s, b_s) = 1 \text{ and } deg\ g_s(x_1, x_2, \cdots, x_{s+1}) < \min\{a_s, b_s\}.$$

Let a point $p = (i_1, i_2, \cdots, i_n)$ in R^n represent a monomial $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. we define the weight of the monomial as follows:

Definition 4.1 *For a n-dimensional monomial $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, we define its weight as*

$$w(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}) = \sum_{j=1}^{n} \left(\prod_{k=1}^{n-j} b_k \prod_{k=n-j+1}^{n-1} a_k \right) i_j.$$

Example 4.1 *Let $n = 6$, and $a_s = 5, b_s = 4$, for $s = 1, 2, \cdots, 5$. Based on their weights, we have the following increasing monomial sequence:*

$$H = \{1, x_1, x_2, x_3, x_4, x_1^2, x_1x_2, x_3, x_2^2, x_1x_3, x_2x_3, x_1x_4, x_1^3, x_6, x_3^2, x_2x_4, x_1^2x_2, x_1x_5, \cdots\}$$

For convenience of expression, we consider the Hermitian-like curves over $GF(2^4)$:

$$\begin{cases} x_1^5 + x_2^4 + x_2 = 0 \\ x_2^5 + x_3^4 + x_3 = 0 \\ \cdots\ \cdots\ \cdots \\ x_{n-1}^5 + x_n^4 + x_n = 0 \end{cases} \tag{11}$$

This curve has $N = 4^{n+1}$ rational points. Thus, the code C_r defined by $\mathbf{H}_r$ is an $[4^{n+1}, 4^{n+1} - r]$. For any monomial $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, its weight is defined as

$$w(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}) = \sum_{j=1}^{n} 4^{n-j} 5^{j-1} i_j.$$

When we apply Bezout's theorem to high dimensional cases, we compute the resultants many times, once for one variable only. For example, when we consider curve (11) and polynomials $f_\mu(x_1, x_2, \cdots, x_n)$ for $\mu = 1, 2, \cdots, p$, we first consider the x_1-resultant $R_1(x_2, \cdots, x_{n-1}, x_n)$ of

$$\begin{cases} x_1^5 + x_2^4 + x_2 = 0 \\ f_1(x_1, x_2, \cdots, x_n) = 0 \\ \cdots\ \cdots\ \cdots \\ f_p(x_1, x_2, \cdots, x_n) = 0. \end{cases}$$

Then we consider the x_2-resultant $R_2(x_3, \cdots, x_{n-1}, x_n)$ of

$$\begin{cases} x_2^5 + x_3^4 + x_3 = 0 \\ R_1(x_2, \cdots, x_{n-3}, x_n) = 0. \end{cases}$$

Repeat the above precess, we finally consider the x_{n-1}-resultant $R_{n-1}(x_n)$ of

$$\begin{cases} x_{n-1}^5 + x_n^4 + x_n = 0 \\ R_{n-2}(x_{n-1}, x_n) = 0. \end{cases}$$

Then, following the similar processes in the 3-dimensional cases, we can prove the following results. Our results can be generalized to the codes defined on curve (10).

Lemma 4.1 $D_{\{[x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}]\}} \leq \sum_{j=1}^{n} 4^{n-j} 5^{j-1} i_j$.

Theorem 4.1 $D_p^{(r)} \leq w(\mathbf{h}_r) - w(\mathbf{h}_p)$.

Theorem 4.2 *Let C_r be a $[4^{n+1}, 4^{n+1} - r]$ code defined by parity-check matrix $\mathbf{H}_r = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_r]^T$. Then*

$$d_h(C_r) = h + r, \text{ if } h \geq w(\mathbf{h}_r) - r + 2.$$

Proof: By Theorem 1.1, we know that, if $D_{r-(d-1)+h}^{(r)} < d - 1$, then $d_h(C_r) \geq d$. Let $p = r - (d-1) + h$, then $d - 1 = r - p + h$. When $h \geq w(\mathbf{h}_r) - r + 2$, $r - 1 + h \geq r - 1 + w(\mathbf{h}_r) - r + 2 = w(\mathbf{h}_r) + 1 \geq D_1^{(r)} + 1 > D_1^{(r)}$. This means that $r - 1 + h$ is the first value of $r - p + h$ such that $r - p + h = d - 1 > D_p^{(r)}$, when p takes $1, 2, \cdots, r$. Thus, when $h \geq w(\mathbf{h}_r) - r + 2$,

$$d_h(C_r) \geq d = r - 1 + h + 1 = h + r. \tag{12}$$

On the other hand, however, by the generalized Singleton bound we have

$$d_h(C_r) \leq h + r. \tag{13}$$

From (12) and (13), we have

$$d_h(C_r) = h + r, \text{ if } h \geq w(\mathbf{h}_r) - r + 2.$$

□

Remark 4.1: In [16] and [6], a similar result was given for the AG codes form Hermitian curves. Our result is on the AG codes from Hermitian curves in high dimensional spaces, and our approach does not need Riemann-Roch theorem.

Example 4.2 *Consider polynomials in the four-dimensional space. WE have the following monomial series*

$$\begin{aligned} H \;=\; & \{1, x_1, x_2, x_3, x_4, x_1^2, x_1x_2, x_2^2, x_1x_3, x_2x_3, x_1x_4, x_1^3, x_3^2, x_2x_4, \\ & x_1^2x_2, x_1x_2^2, x_3x_4, x_1^2x_3, x_2^3, x_1x_2x_3, x_4^2, x_1^2x_4, x_1^4, x_2^2x_3, \cdots\}. \end{aligned}$$

The corresponding weight series is

$$\begin{aligned} W &= \{0, 64, 80, 100, 125, 128, 144, 160, 164, 180, 189, 192, 200,\\ &\quad 205, 208, 224, 225, 228, 240, 244, 250, 253, 256, 260, \cdots\}. \end{aligned}$$

Let

$$\mathbf{H}_r = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_r]^T.$$

The code C_r defined by check parity matrix $\mathbf{H}_r$ is a $[4^5, 4^5 - r]$ code.

If we take $r = 8$, then $w(\mathbf{h}_r) - r + 2 = w(\mathbf{h}_8) - 8 + 2 = 160 - 8 + 2 = 154$. By Theorem 4.2, we have

$$d_h(C_8) = h + 8, \ \textit{if } h \geq 154.$$

For example, $d_{154}(C_8) = 162, d_{200}(C_8) = 208$.

When $r = 16$, we have $w(\mathbf{h}_r) - r + 2 = w(\mathbf{h}_{16}) - 16 + 2 = 224 - 16 + 2 = 210$. By Theorem 4.2, we have

$$d_h(C_{16}) = h + 16, \ \textit{if } h \geq 210.$$

For example, $d_{210}(C_{16}) = 224, d_{300}(C_{16}) = 316$.

5 Construction of Some Codes in High Dimensional Spaces

In the is section, we are going to give some examples to show how to use Bezout's Theorem and the results in the above sections to construct more efficient codes in high dimensional spaces.

The following is a useful lemma:

Lemma 5.1 *The following system of equations has at most three solutions:*

$$\begin{cases} x^2 + a_1x + b_1y + c_1 = 0, \\ xy + a_2x + b_2y + c_2 = 0, \\ y^2 + a_3x + b_3y + c_3 = 0, \end{cases}$$

where a_i, b_i, and c_i are arbitrary numbers.

Proof: The x-resultant $R(y)$ of the system is determined by the following matrix:

$$\begin{bmatrix} 1 & a_1 & b_1y + c_1 \\ y + a_2 & b_2y + c_2 & 0 \\ 0 & y + a_2 & b_2y + c_2 \\ a_3 & y^2 + b_3y + c_3 & 0 \\ 0 & a_3 & y^2 + b_3y + c_3 \end{bmatrix}.$$

If we just choose the first, the third and the fifth rows of the matrix, we have

$$\begin{bmatrix} 1 & a_1 & b_1y + c_1 \\ 0 & y + a_2 & b_2y + c_2 \\ 0 & a_3 & y^2 + b_3y + c_3 \end{bmatrix}.$$

Thus, $R(y) = y^3 + Ay^2 + By + C$ for some A, B and C. By Bezout's Theorem, the system has at most three solutions. □

5.1 Linear Codes Better Than the Improved Hermitian Codes

Now we consider irreducible Hermitian space curve over $GF(2^2)$:

$$\begin{cases} x^3 + y^2 + y = 0, \\ y^3 + z^2 + z = 0. \end{cases}$$

From the definition, we have $w(x) = 4, w(y) = 6$ and $w(z) = 9$. Based on the weights, we have the following increasing series of monomials:

$$\{1, x, y, x^2, z, xy, x^3, xz, x^2y, yz, x^2z, x^3y, xyz, x^3z, \cdots\}.$$

If we take seven polynomials as $\{1, x, y, x^2, z, xy, xz + yz\}$ and consider $D_4^{(7)}$, we have the following theorem.

Theorem 5.1 $D_4^{(7)} \leq 3$.

Proof:
1) It is easy to check

$$D\{[1], *, *, *\}, D\{[x], *, *, *\}, D\{[y], *, *, *\} \leq 3.$$

2) Now we prove $D\{[x^2], [z], [xy]], [xz+yz]\} \leq 3$. It is equivalent to proving that the following system of equations has at most three solutions:

$$x^3 + y^2 + y = 0, \tag{14}$$
$$y^3 + z^2 + z = 0, \tag{15}$$
$$x^2 + A_1x + B_1y + C_1 = 0, \tag{16}$$
$$z + A_2x + B_2y + C_2 = 0, \tag{17}$$
$$xy + A_3x + B_3y + C_3 = 0, \tag{18}$$
$$xz + yz + A_4x + B_4y + C_4 = 0, \tag{19}$$

Solve (17) for z and substitute it into (19), we have

$$x^3 + y^2 + y = 0, \tag{20}$$
$$y^3 + A_2^2x^2 + B_2^2y^2 + a_2x + B_2y + (C_2^2 + C_2) = 0, \tag{21}$$
$$x^2 + A_1x + B_1y + C_1 = 0, \tag{22}$$
$$xy + A_3x + B_3y + C_3 = 0, \tag{23}$$
$$A_2x^2 + (A_2 + B_2)xy + B_2y^2 + (A_4 + C_2)x + (B_4 + C_2)y + C_4 = 0, \tag{24}$$

Consider the determinant of the coefficient matrix of x^2, xy, y^2 in (22), (23) and (24)

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ A_2 & A_2 + B_2 & B_2 \end{vmatrix} = B_2.$$

When $B_2 \neq 0$, (22), (23) and (24) are equivalent to

$$\begin{cases} x^2 + a_1 x + b_1 y + c_1 = 0, \\ xy + a_2 x + b_2 y + c_2 = 0, \\ y^2 + a_3 x + b_3 y + c_3 = 0, \end{cases}$$

From Lemma 5.1, they have at most three common roots. Thus, (20) - (24), and therefore (14) - (18), have at most three common roots.

When $B_2 = 0$, equations (20) - (24) becomes

$$x^3 + y^2 + y = 0, \tag{25}$$
$$y^3 + A_2^2 x^2 + a_2 x + (C_2^2 + C_2) = 0, \tag{26}$$
$$x^2 + A_1 x + B_1 y + C_1 = 0, \tag{27}$$
$$xy + A_3 x + B_3 y + C_3 = 0, \tag{28}$$
$$A_2 x^2 + A_2 xy + B_2 y^2 + (A_4 + C_2)x + (B_4 + C_2)y + C_4 = 0, \tag{29}$$

If we multiply (26) by A_2^2 and subtract the result from (27), we have

$$y^3 + (A_2 + A_2^2 A_1)x + A_2^2 B_1 y + (C_2^2 + C_2 + C_1) = 0. \tag{30}$$

i) When $(A_2 + A_2^2 A_1) = 0$, we consider (25), (27) and (30). The *x-resultant* $R(y)$ is the following determinant

$$R(y) = \begin{vmatrix} 1 & A_1 & B_1 y + C_1 \\ 0 & y^3 + A_2^2 B_1 y + C' & 0 \\ 0 & 0 & y^3 + A_2^2 B_1 y + C' \end{vmatrix} = y^6 + A_2^4 B_1^2 y^2 + C'^2,$$

where $C' = C_2^2 + C_2 + C_1$.

Since $y^6 = y^3$ in $GF(2^2)$, we have

$$R(y) = y^3 + A_2^4 B_1^2 y^2 + C'^2.$$

By Bezout's theorem, (25), (27) and (30), and therefore (25) - (29), have at most three common roots.

ii) When $(A_2 + A_2^2 A_1) \neq 0$, we solve (30) for x and get

$$x = ay^3 + by + c, \tag{31}$$

where $a = 1/(A_2 + A_2^2 A_1) \neq 0, b = A_2^2 B_1/(A_2 + A_2^2 A_1)$, and $c = (C_2^2 + C_2 + C_1)/(A_2 + A_2^2 A_1)$. If $b = 0$, substitute $x = ay^3 + c$ into (25), we have

$$(a^3 + b^3 + a^2 c + ac^2)y^3 + y^2 + y + c^3 = 0. \tag{32}$$

Obviously, equation (32) has at most three solutions.

If $b \neq 0$, substitute $x = ay^3 + by + c$ into (27), we have

$$(a^2 + A_1)y^3 + b^2 y^2 + (B_1 + aA_1)y + (c^2 + C_1 + cA_1) = 0. \tag{33}$$

Since $b^2 \neq 0$, equation (33) has at most three solutions. Thus, (25) - (29), and therefore (14) - (18), have at most three common roots. □

From Riemann-Roch Theorem, the AG code with $d \geq 5$ should have $r = d + g - 1 = 10$. This means that the AG code with $d \geq 5$ is (16, 6, $\geq$ 5). In [10], an improved AG code (16, 8, $\geq$ 5) was given. Using Theorem 5.1, a better AG code can be constructed by taking $\mathbf{H} = [1, x, y, x^2, z, xy, xz + yx]^T$. The new code is linear code (16, 9, $\geq$ 5). It has more information bits and therefore is more efficient.

5.2 More Efficient Double-byte Error-correcting Codes

Consider finite field $GF(q^3) = GF(4^3)$. Let β be a primitive element of $GF(q^3)$. Then $GF(q^3) = GF(2^6) = \{0, 1, \beta, \beta^2, \cdots, \beta^{61}, \beta^{62}\}$. Suppose $\alpha = \beta^{21}$, then $GF(q) = GF(4) = \{0, 1, \alpha, \alpha^2\}$. We know that $[GF(q^3) : GF(q)] = 3$, $GF(q^3)$ is a 3-dimensional vector space over $GF(q)$. We can prove that for any $a_0, a_1, a_2 \in GF(q) = \{0, 1, \alpha, \alpha^2\}$, $a_0 + a_1\beta + a_2\beta^2 = 0$ if and only if $a_0 = a_1 = a_2 = 0$, i.e., $1, \beta, \beta^2$ are linear independent over $GF(q)$. So $1, \beta, \beta^2$ is a basis of $GF(q^3)$ over $GF(q)$. Let x, y, z be variables. Then, $(x + y\beta + z\beta^2)^{q+1} = g_0(x, y, z) + g_1(x, y, z)\beta + g_2(x, y, z)\beta^2$, where

$$\begin{aligned} g_1(x, y, z) &= x^2 + \alpha xy + \alpha^2 y^2 + yz + \alpha xz + z^2, \\ g_2(x, y, z) &= \alpha^2 y^2 + yz + \alpha^2 xz + \alpha yz + \alpha z^2, \\ g_3(x, y, z) &= xz + \alpha xy + \alpha^2 y^2 + \alpha^2 yz + z^2. \end{aligned}$$

Obviously, $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ are polynomials with three variables and coefficients in $GF(q)$. On the other hand, since

$$((x + y\beta + \beta^2)^{q^2+q+1})^q = (x + y\beta + \beta^2)^{q^2+q+1},$$

$(x + y\beta + \beta^2)^{q^2+q+1}$ is also a polynomial with coefficients in $GF(q)$.

Now let $\mathbf{h}_1 = 1, \mathbf{h}_2 = x, \mathbf{h}_3 = y, \mathbf{h}_4 = z, \mathbf{h}_5 = g_0(x, y, z), \mathbf{h}_6 = g_1(x, y, z), \mathbf{h}_7 = g_3(x, y, z), \mathbf{h}_8 = (x + y\beta + \beta^2)^{q^2+q+1}$. For any polynomial $\mathbf{h}_i$,we define its evaluated vector as $\mathbf{h}_i = (\mathbf{h}_i(P_1), \mathbf{h}_i(P_2), \cdots, \mathbf{h}_i(P_{64}))^T$, where $P_1, P_2, \cdots, P_{64}$ are the 64 points in $GF(q^3)$, when $GF(q^3)$ is considered as a three-dimensional vector space over $GF(q)$. Let $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_8]^T$. Then we have a code with parameters:

$$n = q^3 = 64, k = 56.$$

By the following theorem, we know that C is an (64,56, $\geq$5) code.

Theorem 5.2 *Let* $\mathbf{H} = [1, x, y, z, g_0(x, y, z), g_1(x, y, z), g_3(x, y, z), (x + y\beta + \beta^2)^{q^2+q+1}]^T$. *Then* $D_5^{(8)} \leq 3$.

Proof: Let $D_5^{(8)} = D_{\{[\mathbf{h}_{\lambda_1}],[\mathbf{h}_{\lambda_2}],[\mathbf{h}_{\lambda_3}],[\mathbf{h}_{\lambda_4}],[\mathbf{h}_{\lambda_5}]\}}$.

It is easy to check that

$$\begin{aligned} D_{\{[1],[*],[*],[*],[*]\}} &= 0 \leq 3, \\ D_{\{[x],[*],[*],[*],[*]\}} &\leq 3, \\ D_{\{[y],[*],[*],[*],[*]\}} &\leq 3. \end{aligned}$$

Thus, it is sufficient to prove the following system of equations has at most three distinct solutions:

$$\begin{cases} z + A_1x + B_1y + C_1 = 0, \\ g_0(x,y,z) + A_2x + B_2y + C_2 = 0, \\ g_1(x,y,z) + A_3x + B_3y + C_3 = 0, \\ g_2(x,y,z) + A_4x + B_4y + C_4 = 0, \\ (x + y\beta + z\beta^2)^{q^2+q+1} + A_5x + B_5y + C_5 = 0. \end{cases} \tag{34}$$

Substitute $z = A_1x + B_1y + C_1$ into $(x + y\beta + z\beta^2)^{q^2+q+1}$, and consider its part of degree 2, which is $((1 + A_1\beta^2)x + (\beta + B_1\beta^2)y)^{q+1} = (1 + A_1\beta^2)^{q+1}(x + y\frac{\beta+B_1\beta^2}{1+A_1\beta^2})^{q+1}$. Because $1 + A_1\beta^2 \neq 0$, divide it by $(1 + A_1\beta^2)^{q+1}$ and let $c = \frac{\beta+B_1\beta^2}{1+A_1\beta^2} \in GF(q^3)$. Then $(x + cy)^{q+1} = x^2 + (c^q + c)xy + c^{q+1}$. Suppose that $c^q + c = g_0 + g_1\beta + g_2\beta^2$, $c^{q+1} = h_0 + h_1\beta + h_2\beta^2$, then $(x + y\beta)^{q+1} = (x + g_0xy + h_0y^2) + (g_1xy + h_1y^2)\beta + (g_2xy + h_2y^2)\beta^2$. Thus, (34) is equivalent to the following system of equations:

$$\begin{cases} z + A_1x + B_1y + C_1 = 0, \\ x + g_0xy + h_0y^2 + A_2'x + B_2'y + C_2' = 0, \\ g_1xy + h_1y^2 + A_3'x + B_3'y + C_3' = 0, \\ g_2xy + h_2y^2 + A_4'x + B_4'y + C_4' = 0, \\ (x + y\beta + z\beta^2)^{q^2+q+1} + A_5x + B_5y + C_5 = 0. \end{cases} \tag{35}$$

If we can prove the following determinant is not zero, then there are three equations in (35) such that the system of them is equivalent to the system of equations considered in Lemma 5.1. Then, by Lemma 5.1, we know that (35) has at most three distinct solutions.

$$\begin{vmatrix} 1 & g_0 & h_0 \\ 0 & g_1 & h_1 \\ 0 & g_2 & h_2 \end{vmatrix} = \begin{vmatrix} g_1 & h_1 \\ g_2 & h_2 \end{vmatrix}.$$

If it is zero, then there exist a nonzero element $a \in GF(q)$ such that $(h_1, h_2) = (g_1, g_2)$. So we have $c^{q+1} + ac^q + ac = h_0 + ag_0 = b \in GF(q)$, and $(c^{q+1} + ac^q + ac)^q = b^q = b$, i.e., $c^{q^2+q} + ac^{q^2} + ac^q = b$. Add the above formulas, we obtain $c^{q^2+q} + c^{q+1} + ac^{q^2} = ac$, so

$$a = \frac{c^{q^2+q} + c^{q+1}}{c^{q^2} + c} = c^q.$$

So $c^{q^2} = (c^q)^q = a^q = a = c^q, c^{q^3} = (c^{q^2})^q = (c^q)^q = c^{q^2} = c^q$. On the other hand, $c \in GF(q^3)$, so $c^{q^3} = c$ and therefore, $c^q = c, c \in GF(q)$, but $c = \frac{\beta+B_1\beta^2}{1+A_1\beta^2}$, and $1, \beta, \beta^2$ is a basis of $GF(q^3)$. This is impossible. So the proof is completed. □

Remark 5.1: In Theorem 7 in [17], Dumer constructed a class of codes over $GF(q)$, where q is a power of an odd prime. The minimum distances of these codes are greater than or equal to 5. According to Dumer, when $n = q^3$, the codes have the following parameters:

$$n = q^3, r = 8, d \geq 5.$$

These codes are known to be optimal in the sense that no other codes with $d \geq 5$ and the sane code lengths have fewer number of parity checks. But, unfortunately, these codes are defined only on $GF(q)$ for odd prime number q. Our code C has the same parameters and is defined on $GF(2^3)$.

6 Conclusions

Bezout's theorem was used to determine an upper bounds of the numbers of common points of two-dimensional polynomials in [1]. With the upper bounds, lower bounds of the minimum distance and generalized Hamming weights of linear codes were also given in [1]. In this paper, we generalize the results in [1] to n-dimensional spaces. we not only give the upper bounds on the number of the intersection points of n-dimensional polynomials and the lower bounds on the generalized Hamming weights, but also give the exact values of the generalized Hamming weights $d_h(C_r)$ for large enough h. With the results in this paper, new methods for constructing more efficient linear codes can be built. They will be applied in computer memory systems, distributed systems [14, 15], CD audio, Video disk, and CD ROM.

References

[1] Gui-Liang Feng, T. R. N. Rao and Gene A. Berg, "Generalized Bezout's Theorem and Its Applications in Coding Theory", to appear.

[2] Gui-Liang Feng, T. R. N. Rao, "A Class of Algebraic Geometric Codes from Curves in High-Dimensional Projective Spaces", Lecture Notes in Computer Science 673, Springer-Verlag, pp. 132-146, 1993.

[3] R. E. Blahut, *Theory and Practice of Error Control Codes*, Reading, Ma: Addison-Wesley, 1985.

[4] V. K. Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. on Information Theory*, Vol. IT-37, pp. 1412-1428, Sept., 1991.

[5] J. W. P. Hirschfeld, M. A. Tsfasman, and S. G. Vladut, "The Weight Hierarchy of Higher Dimensional Hermitian Codes," *IEEE Trans. on Information Theory*, Vol. 40, pp. 275-278, January 1994.

[6] K. Yang, P. V. Kumar, and H. Stichtenoth, "On the Weight Hierarchy of Geometric Goppa Codes," *IEEE Trans. on Information Theory*, Vol. IT-40, pp. 913-920, May 1994.

[7] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, The American Mathematical Society, 1990.

[8] J.J. Sylvester, "On a general method of determining by mere inspection the derivations from two equations of any degree", *Philosophical Magazine*, 16(1840), 132-135.

[9] G. L. Feng and T. R. N. Rao, "A Simple Approach for Construction of Algebraic Geometric Codes from Affine Plane Curves," *IEEE Trans. on Information Theory*, Vol. IT-40, No.4, pp. 1003-1012, July 1994.

[10] G. L. Feng and T. R. N. Rao, "Improved Geometric Goppa Codes, Part I: Basic Theory" to appear in *IEEE Trans. on Information Theory.*

[11] S. Miura and N. Kamiya, "Geometric-Goppa Codes on Some Maximal Curves and Their Minimum Distance," *Proceedings of 1993 IEEE Information Theory Workshop*, June 4-8, 1993 at Shizuoka, Japan, pp. 85-86.

[12] S. Kaneda and E. Fujiwara, "Single byte error correcting-double byte error detecting codes for memory systems," *IEEE Trans. on Computers*, Vol. C-31, pp.596-602, July, 1982.

[13] C. L. Chen, "Byte-oriented error-correcting codes for semiconductor memory systems," *IEEE Trans. on Computers*, Vol. C-35, pp.646-648, July, 1986.

[14] M. O. Rabin, "Efficient dispersal of information for security, load balancing and fault-tolerance," Harvard University, Cambridge, MA. TR-02-87, Apr. 1987.

[15] G. Agrawal and P. Jalote, "Coding-based replication schemes for distributed systems," *IEEE Trans. on Parallel and Distributed Systems*, Vol. 6, pp. 240-251, Mar. 1995.

[16] Carlos Munuera, "On the Generalized Hamming Weights of Geometric Goppa Codes," *IEEE Trans. on Information Theory*, Vol. 40, No. 6, pp. 2092-2099, 1994.

[17] I. Dumer, "Nonbinary double-error-correcting codes designed by means of algebraic varieties," *IEEE Trans. on Information Theory*, Vol. IT-41, No. 6, PP. 1657-1666, 1995.